Startup

Note de la rédaction

La REE s'efforce depuis le numéro 2021-4 de présenter sous une forme synthétique dans cette nouvelle rubrique les caractéristiques de quelques startups implantées sur le territoire national qui méritent selon nous l'attention de nos lecteurs pour la qualité de l'innovation que ces jeunes entreprises mettent sur le marché et les emplois qu'elles créent, contribuant ainsi à la vitalité économique du pays.

Afin d'enrichir le vivier d'entreprises susceptibles d'être ainsi mises en valeur dans notre Revue, la REE sollicite les responsables de jeunes pousses créées entre 2014 et 2020 pour qu'ils adressent au fil de l'eau le descriptif de leur entreprise (demander le modèle à remplir à : **redacree@see.asso.fr**) pour insertion éventuelle dans un prochain numéro de la REE.

Une priorité sera donnée par le comité de rédaction aux startups ayant déjà été reconnues par l'attribution de prix ou reconnaissances diverses ou dont les produits ont été exposés dans des salons internationaux (CES par exemple).

Dans ce numéro, nous vous proposons exceptionnellement un cahier constitué de 6 start-up proposant toutes des produits innovants destinés à garantir la cybersécurité de leurs clients, thème qui est développé dans le dossier principal du numéro.

ASTRAN
CYBERSÉCURITÉ

Type de société : SAS
75017 Paris
www.astran.io

Année de création : 2021

Fondateurs :
Fondateurs Yosra Jarraya CEO, **Gilles Seghaier** CTO et **Yahya Jarraya** CCO

Taille de l'équipe :
16 personnes

Présentation :
Astran est un éditeur de logiciels français spécialisé en résilience et sécurité des données. La solution d'Astran, le Continuity Cloud, permet aux entreprises de maintenir leurs activités critiques pendant une cyberattaque majeure, apportant une nouvelle vision plus efficace de la continuité d'activité fondée sur le concept de *Minimum Viable Company*. Cela permet de réduire considérablement les impacts financiers d'une cyberattaque.

La résilience apportée par la solution Astran est renforcée par une technologie brevetée de cryptographie à seuil, en cours de standardisation par le NIST. Astran est également en phase finale de certification CSPN auprès de l'ANSSI et a été sélectionnée en février 2024 par les services du Premier Ministre pour le dispositif France 2030.

Les clients d'Astran incluent Eiffage, Vinci et Sanofi, ainsi que d'autres entreprises majeures qui souhaitent maintenir la confidentialité. « *Grâce à Astran, nous sommes opérationnels dans l'heure suivant une interruption totale de notre système d'information. Cela nous permet de continuer à servir nos clients et de gagner du temps pour rétablir nos systèmes.* » — Cédric Jublot, Eiffage.

Plateforme Astran :
Le socle de la plateforme Astran, nommé S5, est une solution de stockage cyber-résiliente. Elle repose sur des algorithmes cryptographiques avancés qui encodent et fragmentent les données, suivis d'un stockage décentralisé de ces fragments auprès de différents fournisseurs cloud. Les données fragmentées sont ainsi réparties entre plusieurs fournisseurs de cloud (par exemple, français, européens et américains), rendant physiquement impossible la reconstitution des données sans autorisation. Cette innovation technologique offre une sécurité maximale (post-quantique) et une résilience complète, sans nécessité de clé de chiffrement.

• Protection contre les ransomwares
Astran permet aux entreprises de se prémunir contre les ransomwares, combinant résilience et confidentialité des données. De plus, elle offre un niveau de souveraineté inédit en protégeant les données des dispositions du Cloud Act américain, qui permet aux autorités américaines d'accéder aux données stockées chez Amazon, Microsoft et Google. Le mécanisme de fragmentation utilise une intelligence basée sur la notion de seuil, permettant de se passer de certains fragments en cas d'indisponibilité d'un ou plusieurs fournisseurs de cloud sous-jacents. Cela garantit non seulement un niveau de sécurité maximale, mais aussi une disponibilité constante, rendant la plateforme Astran insensible aux ransomwares.

• Intégration transparente et conformité
La solution intègre de façon transparente divers clouds, éliminant ainsi les complexités des méthodes de chiffrement traditionnelles. Elle offre un accès simple et convivial via une API compatible S3 et une interface graphique (Web App). La solution est conforme aux réglementations RGPD et NIS2.

Basée sur ce socle solide, permettant aux entreprises de sanctuariser les procédures et données vitales en cas de crises majeures (comme une interruption due à un ransomware), Astran introduit A.R.I.A (*Astran Resilience Intelligent Assistant*). Cette innovation assure l'excellence opérationnelle au moment le plus critique, garantissant l'efficience et la satisfaction des clients finaux.

La solution Astran est l'approche la plus élégante pour garantir la disponibilité et la sécurité de vos données critiques, à tout moment, de manière simple et efficace, même en cas de défaillance totale de votre système IT.

Reconnaissances et certifications :
Astran a obtenu le ECSO European CISO Choice Award en 2024 et est en cours de certification par l'ANSSI. Elle fait également partie du programme d'accélération de l'État pour l'obtention de la certification SecNumCloud, annoncée en février 2024.

Marchés visés :
• Les entreprises qui ne peuvent pas se permettre une interruption d'activité : Astran assure une disponibilité continue des données, même en cas de défaillance totale du système IT, garantissant ainsi la continuité des opérations et la satisfaction des clients.

• Les entreprises souhaitant se prémunir des attaques de ransomware sur les données de l'entreprise : Astran offre une solution robuste pour protéger les données contre les ransomwares, garantissant résilience et confidentialité.

• Les entreprises contraintes d'utiliser des solutions privées pour garantir la confidentialité de leurs données : jusqu'à présent, ces entreprises ne pouvaient pas utiliser les clouds publics en raison du caractère très sensible de leurs données. Astran leur permet de bénéficier des avantages des clouds publics tout en assurant une sécurité et une confidentialité optimales.

Date de la première commercialisation :
Avril 2022

Levée de fonds /Tours de table effectués et financement :
Plus de 11M€ levés
2M€ pre-seed 2021
5M€ seed 2023

HACKUITY

CYBERSÉCURITÉ

Type de société : SAS
69009 Lyon
www.hackuity.io

Origine de la start-up :
Fondée par trois anciens cadres dirigeants d'Orange Cyberdéfense, se focalisant sur la prévention des cyberattaques.

Année de création : 2020, lancement du produit

Fondateurs :
Patrick Ragaru, **Pierre Polette**, **Pierre Samson**

Taille de l'équipe, taux de croissance prévu :
40+ clients, 50+ employés, croissance annuelle à 3 chiffres depuis 3 ans

Informations techniques :
80 % des cyberattaques utilisent des vulnérabilités publiées il y a une demi-décennie, ce qui montre la difficulté pour les équipes de cybersécurité de suivre et remédier les vulnérabilités connues. Hackuity se focalise sur la gestion des vulnérabilités selon leur risque (*Risk Based Vulnerability Management* - RBVM) avec une solution permettant de collecter l'ensemble des CVE (*Common Vulnerabilities and Exposures*) et des actifs d'une organisation, pour les contextualiser et les prioriser automatiquement via un algorithme propriétaire. Ainsi, les 240 000 failles de sécurité potentielles sont hiérarchisées, ce qui permet d'identifier les quelques dizaines ou centaines de failles qui représentent les menaces les plus importantes pour l'entreprise et qui nécessitent une action de remédiation prioritaire.
La plateforme Hackuity permet de briser les silos de sécurité et fournit une vue unifiée de l'exposition aux attaques cyber spécifique à la surface d'attaque de l'entreprise. Cela permet de remédier aux menaces réelles, plus rapidement. C'est la base d'un *Vulnerability Operation Center* (VOC), cockpit de pilotage des vulnérabilités de l'entreprise.
La plateforme agrège plus de 80 outils leaders du marché en une vision globale et à jour des vulnérabilités. Cela couvre des domaines techniques différents comme pour la gestion des Directory d'entreprise, l'IoT, l'infrastructure, la sécurité applicative, le cloud comme AWS d'Amazon ou le renseignement comme Orange Cyber Defense ou Mandiant (Google).
Hackuity a été distingué en 2021 par le FIC (Forum international de la cybersécurité de Lille). Hackuity a également remporté le Grand Défi organisé par le gouvernement français (2023, 2021). Hackuity a été nominé dans la catégorie Best Vulnerability Management Solution aux SC Awards Europe (2024).

Originalité par rapport à l'existant :
D'une part une vision large et mise à jour des vulnérabilités existantes, d'autre part une priorisation basée sur la surface d'attaque spécifique de l'entreprise.
Hackuity vient d'intégrer Campus Cyber, qui accueille des détachements d'institutions publiques, tels que l'ANSSI (Agence nationale de la sécurité informatique) et la DGSI, ainsi que des startups et des entreprises du secteur.

Hackuity est certifié SOC 2 Type II et accrédité IMDA.

Marchés visés :
Les moyennes et grandes entreprises soucieuses d'améliorer leur pratique de prévention des menaces cybersécurité avec un programme de gestion des vulnérabilités informatiques plus mature.

Date de la première commercialisation : 2020

Levée de fonds :
15M€+ (Series A + Seed) :
Tour de table 12 millions d'euros en mai 2022, pour accélérer nos innovations technologiques et les commercialiser à l'international, avec un focus sur les marchés UK et APAC, via une équipe basée à Singapour.

HARFANGLAB
CYBERSÉCURITÉ

Type de société : SAS
92800 Puteaux
https://harfanglab.io

Année de création : 2018

Fondateurs :
Fondateurs : Grégoire Germain (CEO), **Xavier Boreau** (CFO)**, Maxime Rameau** (CPO) **et Mathieu Gaspard** (directeur R&D)

Taille de l'équipe :
environ 100 collaborateurs

Origine de la start up :
Création par des anciens de l'ANSSI et du ministère des armées.

Informations techniques :
L'entreprise est spécialisée dans la sécurité des terminaux et édite une offre de solutions complète pour la détection et le blocage des cybermenaces connues et inconnues. HarfangLab a conçu une solution ouverte dite EDR (*Endpoint Detection & Response*) conçue pour détecter et bloquer les cyberattaques sur le parc informatique des entreprises. Grâce à ses 5 moteurs de détection complémentaires, dont un à base d'IA, et un spécialisé dans la détection des rançongiciels, Harfanglab est aujourd'hui l'un des acteurs les plus performants du marché, comme l'attestent les résultats des Evaluations MITRE de 2023.

Cette solution est la première à avoir été certifiée par l'ANSSI.
Elle permet de détecter et de bloquer les menaces connues et inconnues sur les terminaux en s'appuyant sur l'analyse comportementale, l'apprentissage automatique et la corrélation des événements. Une solution EDR est complémentaire à l'antivirus, solution également proposée par HarfangLab. Alors que l'antivirus va travailler de manière autonome sur les postes de travail pour détecter les menaces sur une base de signatures (menaces connues), un EDR peut détecter des menaces encore inconnues en corrélant les données des terminaux, détectant les comportements suspects et bloquant l'attaque en redescendant l'information aux autres terminaux.
Cette solution SaaS peut fonctionner sur n'importe quel cloud, et fonctionne aussi on-premise (sur site client).

Originalité par rapport à l'existant :

La solution proposée :
• couvre aussi les menaces inconnues, notamment à l'aide du machine learning ;

• dispose d'une équipe dédiée à la recherche en cybersécurité permettant de contribuer à l'effort collectif de renseignement et de lutte contre les cybermenaces ;

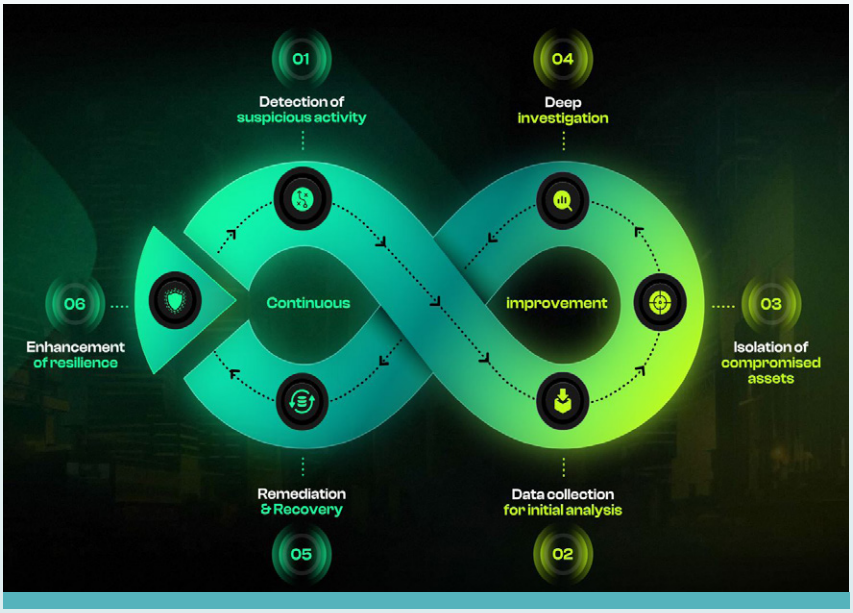
• est la solution la plus ouverte du marché, permettant aux entreprises de construire leur offre cyber la plus en ligne avec leur besoin en connectant d'autres technologies à l'EDR Harfanglab ;

• permet aux clients de conserver leur autonomie stratégique en choisissant leur environnement de confiance (SecNumCloud, Cloud privé, cloud public, *on-premise*).

Marchés visés :
Commercialisation en modèle 100 % indirect via des opérateurs de services de cybersécurité, équipés d'un SOC.
Marchés prioritaires : les PME, les collectivités territoriales, hôpitaux et secteur public, l'industrie de la Défense.

Date de la première commercialisation :
Logiciel aujourd'hui déployé sur plus de 1 million de *endpoints* (postes de travail, postes protégés).

Levée de fonds / Tours de table effectués et financement :
La start-up en pleine croissance avait levé 5 millions d'euros en 2021.
En octobre 2023, elle a levé une série A de 25 millions € auprès du Crédit Mutuel Innovation, Elaia et Mass Mutual Venture, pour attaquer l'international, en particulier en Europe (d'abord Allemagne, puis Autriche, Suisse, Benelux).



IDAKTO

CYBERSÉCURITÉ

Type de société : SAS
78280 Guyancourt
www.idakto.com

Année de création :
2019

Fondateurs :
Hassan Maad, CEO
Marc Loutrel, Directeur des opérations
Yann Bouan, Directeur de la stratégie

Taille de l'équipe :
50 employés en 2024, taux de croissance de 60 %/an

Origine de la start up :
iDAKTO a été créée en 2019 pour sécuriser et simplifier les interactions digitales entre utilisateurs et fournisseurs de services publics ou privés. Notre pari est de proposer une solution permettant de passer de l'identité physique à une identité numérique réutilisable et souveraine. La société a été fondée par Hassan Maad, expert reconnu dans l'identité et l'IAM (*Identity and Access Management*). Hassan Maad a vendu sa première startup, Enatel à Bull/Atos où il devint DG d'Evidian, leader mondial de l'Identity Access Management. Il rejoint ensuite IDEMIA en tant que VP EMEA puis VP Stratégie pour la division identité avant de repartir dans l'entreprenariat avec iDAKTO.

Informations techniques :
iDAKTO est une *scale-up leader* sur l'identité numérique. Ses solutions sont déployées mondialement auprès de gouvernements et de grandes institutions, pour leur garantir des relations de confiance avec leurs utilisateurs.
Le Maroc, la France et la Banque Centrale d'Egypte ont déjà choisi les solutions iDAKTO pour déployer leur portefeuille électronique d'identité numérique. La société permet ainsi à 200 millions d'utilisateurs de disposer d'une identité digitale à valeur légale, assurant un accès simple, sécurisé et inclusif aux services en ligne.

La plateforme d'identité digitale d'IDAKTO permet de gérer le cycle de vie complet de l'identité, depuis sa vérification initiale jusqu'à sa gouvernance. Ses solutions permettent une authentification multi-facteurs inclusive où les fournisseurs de services peuvent choisir parmi plusieurs méthodes d'authentification sécurisées :
• lecture de la carte d'identité avec NFC,
• PIN,
• mot de passe,
• mot de passe à usage unique (fourni par l'application mobile, ou par SMS ou email),
• reconnaissance biométrique faciale ou par empreintes digitales.

iDAKTO est le partenaire technologique de France Identité Numérique qui vise à dématérialiser les documents d'identité pour un usage de services en ligne avec un niveau élevé d'assurance au sens de la réglementation Européenne eIDAS. Les applications Android et iOS France Identité Numérique ont obtenu la certification CSPN (Certification de Sécurité Premier Niveau) de l'ANSSI, ce qui permet de prouver son identité en ligne de façon simple et irréfutable, sans avoir besoin d'envoyer des photos de ses documents d'identité mais aussi ouvre la voie à la dématérialisation jusqu'ici impossible de processus comme la demande de procuration.

iDAKTO fournit toute la couche de sécurité des applications et la plateforme derrière ce qui sera bientôt le portefeuille numérique européen (#EUDIWallet).

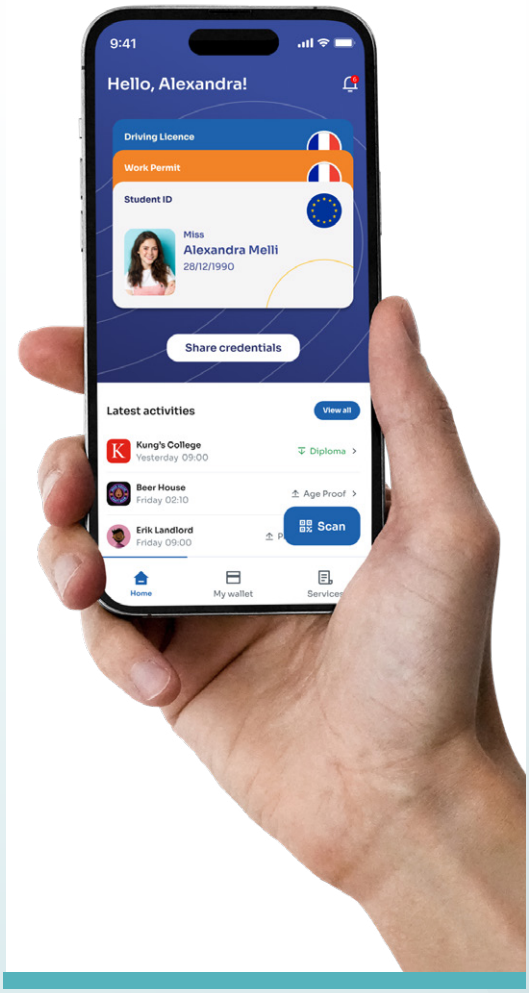
iDAKTO est lauréat du Prix de la recherche du Forum InCyber 2024.

Originalité par rapport à l'existant du marché :
Détention de 8 brevets en cybersécurité et cryptographie.
Utilisé par France Identité Numérique qui forme la base du futur portefeuille numérique européen.

Marchés visés :
B2G (*Business to Government*) et B2B

Date de la première commercialisation :
iDAKTO a été sélectionnée en 2021 pour développer l'application France Identité Numérique. Notre société a également livré en 2022 l'identité digitale du Maroc.

Levée de fonds / Tours de table effectués et financement :
La société est à ce jour autofinancée.



PROVENRUN

CYBERSÉCURITÉ
Type de société : SAS
75017 Paris
https://provenrun.com

Origine de la start up :

Dominique Bolignano a créé ProvenRun en 2009 après avoir cédé Trusted Logic, sa précédente entreprise, à Gemalto.

Fondateurs et principaux responsables :

Dominique Bolignano, Fondateur et Président
Thierry Chesnais, CEO

Taille de l'équipe :

60 personnes

Informations techniques :

ProvenRun part du fait que la confiance est la base essentielle d'un système IoT.
Concentré sur une approche de « sécurité par conception » dans la durée, plutôt que de réaction aux attaques, les produits ProvenRun permettent aux industriels et aux fabricants de dispositifs IoT d'atteindre un niveau de cybersécurité de premier ordre, de développer et de certifier des applications plus rapidement, de prendre de l'avance sur les futures exigences réglementaires, et de réduire considérablement les coûts de maintenance tout au long du cycle de vie de leurs produits.
ProvenRun vise particulièrement les secteurs critiques comme l'aérospatiale, la défense, l'automobile, ou les semi-conducteurs. Ses solutions logicielles sécurisées dès la conception répondent aux défis liés à la croissance rapide de l'IoT. ProvenRun est par exemple un partenaire essentiel dans l'intégration de la sécurité logicielle embarquée pour les Software Defined Vehicles chez les constructeurs et équipementiers automobiles, ainsi que pour les microcontrôleurs chez les fabricants de puces tels que STMicroelectronics.

Les principaux produits de ProvenRun :
ProvenCore : un système d'exploitation sécurisé avancé dans le cadre d'un environnement d'exécution de confiance (*Trusted Execution Environment* TEE) conçu pour fournir une sécurité inégalée pour les objets IoT. ProvenCore est prouvé formellement et certifié Critères Commun EAL7, une première mondiale pour un système d'exploitation.
ProvenCore-M : un système d'exploitation temps réel hautement sécurisé pour concevoir des solutions IoT de confiance. ProvenCore-M est certifié PSA/SESIP niveau 3.
ProvenApps : des solutions sécurisées et modulaires, disponibles en RUST, conformes aux réglementations et aux normes de sécurité en constante évolution dans l'écosystème IoT. Ces applications de confiance fonctionnent au-dessus de ProvenCore et ProvenCore-M, et permettent d'assurer une conformité continue répondant aux exigences de l'industrie tout au long du cycle de vie des objets IoT.

Originalité par rapport à l'existant :

ProvenCore est le seul système d'exploitation certifié au niveau le plus élevé (EAL7) des Critères Communs, la norme mondiale en matière de sécurité informatique.
https://provenrun.com/provencore-secure-os-achieves-eal7-common-criteria-certification/

Marchés visés :

Focus sur l'industrie y compris les secteurs critiques. Les applications de confiance ont été développées pour une variété de secteurs verticaux, y compris l'automobile, l'aérospatiale et la défense, et l'IoT.

Levée de fonds / Tours de table effectués et financement :

En décembre 2023, levée de fonds en Série A de 15 millions € auprès de Tikehau Capital qui a mené cet investissement en collaboration avec le fonds Definvest du ministère français de la défense (géré par BpiFrance).
https://provenrun.com/provenrun-secures-e15-million-series-a-to-accelerate-its-growth-in-security-by-design-for-the-internet-of-things-iot/

Ce financement permet d'accélérer la feuille de route des produits de ProvenRun, notamment les applications de sécurité automobile et les architectures RISC-V, ainsi que son expansion géographique en Amérique du Nord.

Software	Professional Services	Support
✓ Secure OS and Trusted Execution Environments: ProvenCore, ProvenCore-M, ProvenVisor	✓ Consulting: risk analysis, security architecture, certification support	✓ Product documentation and knowledge base
✓ Trusted Applications	✓ Engineering: Secure Boot, TEE development, trusted application development	✓ Support packages and technical advice from developers, engineers, and architects
✓ Certification kits	✓ Training led by experts in security and embedded software development	✓ Board support packages for Arm and RiscV micro-processors and micro-controllers
✓ Software Development Kit to boost your development of trusted applications in C and Rust		

SYNACKTIV

SYNACKTIV
CYBERSÉCURITÉ

Type de société : SAS
75002 Paris
www.synacktiv.com

Année de création : 2012

Fondateurs et principaux responsables :
Nicolas Collignon, Renaud Feil

Taille de l'équipe, CA :
173 collaborateurs, 26,6 millions euros de CA en 2023

Origine de la société :
Les fondateurs, experts en cybersécurité, ont décidé de créer une société dédiée aux aspects techniques de la cybersécurité offensive. Leur approche leur a permis de hisser Synacktiv parmi les leaders du test d'intrusion, de la recherche de vulnérabilités, du développement d'outils et de la réponse à incidents.

Informations techniques :
Synacktiv a pour objectif d'aider les entreprises à évaluer et améliorer le niveau de sécurité de leur système d'information.
L'entreprise spécialiste des tests d'intrusion et du hacking éthique est une référence française en matière de sécurité offensive. La société évalue la sécurité globale d'une entreprise par des tests en conditions réelles (test d'intrusion/Red team), des audits de sécurité pour évaluer le niveau de maturité en Cybersécurité, du *reverse engineering* sans disposer du code source, le développement de solutions spécifiques et la fourniture d'assistance en cas d'incident de sécurité, notamment avec le CSIRT de Synacktiv. Des formations sont aussi dispensées.

Les produits principaux pour les tests d'intrusion sont :
• **Kraqozorus**, plateforme centralisée de cassage d'empreintes de mots de passe
• **Houdini**, pour réaliser des tests d'intrusion couplés physiques et logiques lors de test Red team en interne
• **Oursin**, plateforme d'attaques par *Spear phishing* (avec l'usurpation d'identité d'un contact)
• **Leakozorus**, plateforme d'agrégation, d'indexation et de recherche des identifiants
Lors de la dernière édition du concours de hacking Pwn2Own à Vancouver, trois chercheurs français de Synacktiv ont réussi à hacker une Tesla Model 3. Cette compétition internationale vise à mettre en évidence de manière éthique des vulnérabilités logicielles jusqu'ici non connues.

Originalité par rapport à l'existant du marché :
Expérience des tests d'intrusion des hackers.

Marchés visés :
Toute société ayant des besoins sérieux en cybersécurité et prête à se faire évaluer et accompagner par une équipe technique de haut niveau pour avoir un niveau de sécurité permettant de faire face à des attaquants compétents et motivés.

Date de la première commercialisation : 2012

Levée de fonds / Tours de table effectués et financement :
Aucune